

Docket No.: 62807-159

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
	:	
Katsuyuki UMEZAWA, et al.	:	Confirmation Number:
	:	
Serial No.:	:	Group Art Unit:
	:	
Filed: January 30, 2004	:	Examiner:
	:	
For: CERTIFICATE MANAGEMENT SYSTEM AND METHOD	:	

**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Mail Stop CPD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:


In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. JP 2003-402401, filed on December 2, 2003.

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY


Keith E. George
Registration No. 34,111

By 16,36,139 for

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 KEG:gav
Facsimile: (202) 756-8087
Date: January 30, 2004

62807-159

~~Senchi, SUSAKE, et al.~~

January 30, 2004
Katsuyuki UMEZAWA, et al.

日本国特許庁 *McDermott, Will & Emery*
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年12月 2日
Date of Application:

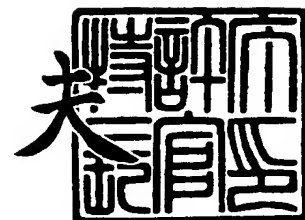
出願番号 特願2003-402401
Application Number:
[ST. 10/C]: [JP 2003-402401]

出願人 株式会社日立製作所
Applicant(s):

2004年 1月19日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2004-3000694

【書類名】 特許願
【整理番号】 K03010081A
【あて先】 特許庁長官殿
【国際特許分類】 G06K 17/00
【発明者】
 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所
 システム開発研究所内
 【氏名】 梅澤 克之
【発明者】
 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所
 システム開発研究所内
 【氏名】 内山 宏樹
【発明者】
 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所
 システム開発研究所内
 【氏名】 洲崎 誠一
【発明者】
 【住所又は居所】 神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所情報
 ・通信グループ内
 【氏名】 児玉 俊臣
【特許出願人】
 【識別番号】 000005108
 【氏名又は名称】 株式会社 日立製作所
【代理人】
 【識別番号】 100075096
 【弁理士】
 【氏名又は名称】 作田 康夫
【選任した代理人】
 【識別番号】 100100310
 【弁理士】
 【氏名又は名称】 井上 学
【手数料の表示】
 【予納台帳番号】 013088
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1

【書類名】 特許請求の範囲**【請求項 1】**

公開鍵証明書の管理システムであって、
提示された公開鍵証明書の有効性を検証し、検証が正しく行えた場合にサービスを提供する、サービス提供者装置と、前記サービス提供者装置が信頼する認証局装置と、ICカードと、からなり、
前記ICカードは、
前記認証局装置に対する証明書を発行するために必要な、第1の秘密鍵とその対となる第1の公開鍵と、前記第1の公開鍵に対して発行された第1の証明書と、
前記サービス提供者装置からサービスを受けるために生成する、第2の秘密鍵とその対となる第2の公開鍵と、
前記第2の公開鍵に対して、前記サービス提供者装置が信頼する前記認証局装置により発行される第2の証明書と、を記憶する記憶部と、
前記第1、第2の公開鍵と第1、第2の秘密鍵とを生成する鍵生成部と、
を備え、
前記認証局装置は、
前記ICカードに対して前記第2の公開鍵の証明書を生成するための、第3の秘密鍵とその対となる第3の公開鍵に対して発行される前記証明書と、を記憶する記憶部と、
発行申請に基づき、第2の公開鍵に対する第2の証明書を生成する証明書生成部と、
を備え、
前記ICカードは、
前記認証局装置による証明書の発行要求に基づき、記憶している前記第1の秘密鍵を用いて、前記認証局装置の証明書を発行する証明書生成部と、
を備える
ことを、特徴とする証明書管理システム。

【請求項 2】

請求項1記載の証明書管理システムであって、
前記認証局装置は、
証明書の失効申請に基づき、証明書の失効情報を生成する失効情報生成部と、
該失効情報生成部で生成した失効情報を保管する失効情報DBと、を備えており、
前記ICカードは、前記サービス提供者装置からサービスを受けるために、
前記第1の証明書と第2の証明書を前記サービス提供者装置に提示し、
前記サービス提供者装置は、
提示された前記第1、第2の証明書の有効性を検証する際に、前記第1の証明書と前記当該第2の証明書の失効情報を、前記認証局装置に問い合わせる証明書検証部、を備える。

【請求項 3】

請求項1記載の証明書管理システムであって、
前記ICカードは、
前記記憶部を、前記サービス提供者固有領域として構成し、
当該固有領域へのアクセスを、前記固有領域に対応する前記サービス提供者装置のみに許可するサービス提供者認証部を備える
ことを特徴とする証明書管理システム。

【請求項 4】

請求項1記載の証明書管理システムであって、
前記ICカードの、前記サービス提供者固有領域、および、証明書生成部に記憶されているデータは暗号化されている
ことを特徴とする証明書管理システム。

【請求項 5】

請求項1記載の証明書管理システムであって、

証明書検証機関装置を備え、

前記証明書検証機関装置は、前記サービス提供者装置の、前記証明書検証部による証明書の有効性検証を、前記サービス提供者装置に代わって行うことを、特徴とする証明書管理システム。

【請求項 6】

請求項 1 記載の証明書管理システムであって、

証明書保管機関装置を備え、

前記証明書保管機関装置は、前記 IC カード内に保存される複数の証明書を前記 IC カードに代わって保管し、要求に従い前記証明書を提供することを、特徴とする証明書管理システム。

【請求項 7】

請求項 2 記載の証明書管理システムであって、

証明書検証時に、

前記認証局装置が前記第 2 の証明書を検証する時に、

前記サービス提供者装置は、チャレンジを送信し、

前記 IC カードは、

前記第 2 の秘密鍵で、前記チャレンジを暗号化し、

該暗号化されたチャレンジと、前記第 2 の秘密鍵に対応した第 2 の証明書と、前記第 1 の秘密鍵に対応した第 1 の証明書と、を前記サービス提供者装置に送信し、

前記サービス提供者装置は、

前記暗号化されたチャレンジを復号化して前記 IC カードに送信した前記チャレンジと一致するかどうかを確認し、

受け取った前記第 1 の証明書と第 2 の証明書との失効情報を取得し、

取得した前記失効情報を用いて、前記第 1、第 2 の証明書の検証処理を行う証明書検証部と、

検証処理において、前記第 1、第 2 の証明書は有効である、と判断した場合に、サービスの提供を行うサービス提供部を備える

ことを特徴とする証明書管理システム。

【請求項 8】

請求項 7 記載の証明書管理システムであって、

前記 IC カードは、

前記記憶部を、前記サービス提供者固有領域として構成し、

前記サービス提供者装置は、前記サービス提供者固有領域へのデータの送受信を行うときに、

前記サービス提供者固有領域との間で、相互認証処理を行うことを特徴とする証明書管理システム。

【請求項 9】

請求項 7 記載の証明書管理システムであって、

前記 IC カードの、前記サービス提供者固有領域、および、証明書生成部へ、データを保存するときに、該データを暗号化した後で、保存することを特徴とする証明書管理システム。

【書類名】明細書**【発明の名称】証明書管理システムおよびその方法****【技術分野】****【0 0 0 1】**

本発明は、ＩＣカード等の記憶媒体を用いた証明書管理方法に関し、さらに詳しくは、複数の証明書がＩＣカード等の記憶媒体に搭載される場合の、証明書失効を効率化するための証明書発行方法に関する。

【背景技術】**【0 0 0 2】**

ＩＣカードに、サービス提供者装置ごとに領域を分けて、アプリケーションおよびデータを搭載する技術が知られている（例えば、非特許文献１参照。）。

【0 0 0 3】

また、ＩＣカードの利用者が公開鍵証明書を申請して取得し、取得した公開鍵証明書がＩＣカードに搭載され、実際に発行されるまでの仕組みを提供している技術もある（例えば、特許文献１参照）。

【0 0 0 4】

また、ＩＣカードに搭載された公開鍵や公開鍵証明書を安全に遠隔より書き換えるため仕組みを提供している技術もある（例えば、特許文献２参照）。

【0 0 0 5】

【特許文献１】特開 2 0 0 2 - 2 9 8 0 8 8 号公報

【0 0 0 6】

【非特許文献１】「グローバルプラットフォームカードスペシフィケーションバージョン 2. 1 (GlobalPlatform Card Specification Version 2.1)」, (米国), グローバルプラットフォーム社 (GlobalPlatform Inc.), 2 0 0 1 年 6 月, p. 2 7

【特許文献２】米国特許出願公開第 2 0 0 3 / 0 0 5 6 0 9 9 A 1 号明細書

【発明の開示】**【発明が解決しようとする課題】****【0 0 0 7】**

サービス提供者装置は、サービス提供時に、サービス利用者に、該サービス提供者装置が信頼する認証局装置から発行された証明書の提示を求め、該証明書が確かに、信頼する認証局装置から発行されたものかどうか、有効期限が切れていないかどうか、等の検証を行うことで、サービス利用者を認証することができる。

【0 0 0 8】

昨今普及しつつあるマルチアプリケーション搭載可能なＩＣカードに、複数のサービス提供者装置が、個別に、証明書および該証明書に対応する秘密鍵を搭載し、認証処理を行う場合を考える。

【0 0 0 9】

個々のサービス提供者装置は、１つの共通の認証局装置だけを信頼するのではなく、個別に認証局装置を信頼したい場合も考えられる。このような場合に、たとえば、ＩＣカードを無くしてしまったため、ＩＣカードの所有者が、ＩＣカードに搭載されているすべての証明書を失効させたい場合、すべてのサービス提供者に、あるいは、認証局に連絡しなければならず、効率が悪い。また、個々のサービス提供者装置が、自らが信頼する認証局装置から発行された証明書を、自らの権限で失効させたい場合もある。

【0 0 1 0】

従って、簡単でかつ柔軟な失効方法が求められている。

【課題を解決するための手段】**【0 0 1 1】**

本発明は、上記事情に鑑みてなされたものであり、一つのサービス提供者装置（たとえばカード発行者等の第１のサービス提供者装置）に連絡し、該サービス提供者装置１が信頼する認証局装置から発行された証明書を失効するだけで、他のサービス提供者装置が信

頼する認証局装置から発行された証明書も同時に失効させることができる、証明書管理方法およびその方法が適用されるシステムを提供する。

【0012】

また、複数のサービス提供者装置が、それぞれ異なる信頼する認証局装置から発行される証明書をICカードに搭載しており、何らかの理由で、ある特定の証明書を失効させたい場合に、他の証明書は失効させずに、上記特定の証明書を個別に失効させることもできる、証明書管理方法およびその方法が適用されるシステムを提供する。

【0013】

具体的には、上位の第1のサービス提供者装置が信頼する第1の認証局装置により発行されたICカード内の第1の証明書を用いて、ICカード内で、下位の第2のサービス提供者装置が信頼する、第2の認証局装置の証明書2'を生成し、さらに該証明書2'を用いて第2の認証局装置が第2の証明書を生成する、という階層的な証明書の連鎖を構成する。

【0014】

このとき、第2のサービス提供者装置が複数で、それぞれ異なる第2の認証局装置を信頼し、複数の第2の認証局装置が、それぞれ第2の証明書を生成してもよい。

【0015】

上記連鎖構成により、該下位の証明書2の有効性を検証するためには、上記証明書2'および上記証明書1の有効性の検証が必要となる。つまり、ICカードを無くした等の理由により、証明書1および証明書2を失効させたい場合、サービス提供者装置1が信頼する認証局装置により発行された上位の証明書1を、失効させるだけで、一つ以上のサービス提供者装置2が信頼する一つ以上の認証局装置2が発行した一つ以上の下位の証明書2も失効させることができる。

【0016】

一方、上記連鎖構成において、各証明書の検証時には、その発行元認証局が発行した失効情報を参照する構成とすることにより、個々の証明書を失効させることも可能である。例えば、サービス提供者装置2がサービスの提供を停止する場合などには、サービス提供者装置2が信頼する認証局装置による失効情報を発行させる。これにより、サービス提供者装置1が信頼する認証局装置1が発行した証明書1は有効のまま、サービス提供者装置2が信頼する認証局から発行された証明書2を、失効させることが可能となる。

【0017】

本発明による証明書管理システムは、より具体的には、提示された公開鍵証明書の有効性を検証し、検証が正しく行えた場合にサービスを提供する、サービス提供者装置と、上記サービス提供者装置が信頼する認証局装置と、ICカードと、からなる。

【0018】

そして、上記ICカードは、上記認証局装置に対する証明書を発行するために必要な、第1の秘密鍵とその対となる第1の公開鍵と、上記第1の公開鍵に対して発行された第1の証明書と、上記サービス提供者装置からサービスを受けるために生成する、第2の秘密鍵とその対となる第2の公開鍵と、上記第2の公開鍵に対して、上記サービス提供者装置が信頼する上記認証局装置により発行される第2の証明書と、を記憶する記憶部と、上記第1、第2の公開鍵と第1、第2の秘密鍵とを生成する鍵生成部と、を備えることを特徴とする。

【0019】

さらに、上記認証局装置は、上記ICカードに対して上記第2の公開鍵の証明書を生成するための、第3の秘密鍵とその対となる第3の公開鍵に対して発行される上記証明書と、を記憶する記憶部と、発行申請に基づき、第2の公開鍵に対する第2の証明書を生成する証明書生成部と、を備えることを特徴とする。

【0020】

さらに、上記ICカードは、上記認証局装置による証明書の発行要求に基づき、記憶している上記第1の秘密鍵を用いて、上記認証局装置の証明書を発行する証明書生成部と、

を備えることを特徴とする。

【0021】

また、上記証明書管理システムにおいて、上記認証局装置は、証明書の失効申請に基づき、証明書の失効情報を生成する失効情報生成部と、該失効情報生成部で生成した失効情報を保管する失効情報DBと、を備え、上記ICカードは、上記サービス提供者装置からサービスを受けるために、上記第1の証明書と第2の証明書を上記サービス提供者装置に提示し、上記サービス提供者装置は、提示された上記第1、第2の証明書の有効性を検証する際に、上記第1の証明書と上記当該第2の証明書の失効情報を、上記認証局装置に問い合わせる証明書検証部、を備えることを特徴とする。

【0022】

また、上記証明書管理システムにおいて、証明書検証時に、上記認証局装置が上記第2の証明書を検証する時に、上記サービス提供者装置は、チャレンジを送信し、上記ICカードは、上記第2の秘密鍵で、上記チャレンジを暗号化し、該暗号化されたチャレンジと、上記第2の秘密鍵に対応した第2の証明書と、上記第1の秘密鍵に対応した第1の証明書と、を上記サービス提供者装置に送信し、上記サービス提供者装置は、上記暗号化されたチャレンジを復号化して上記ICカードに送信した上記チャレンジと一致するかどうかを確認し、受け取った上記第1の証明書と第2の証明書との失効情報を取得し、取得した上記失効情報を用いて、上記第1、第2の証明書の検証処理を行う証明書検証部と、検証処理において、上記第1、第2の証明書は有効である、と判断した場合に、サービスの提供を行うサービス提供部を備えることを特徴とする。

【発明の効果】

【0023】

本発明によれば、複数のサービス提供者装置が、それぞれ異なる信頼する認証局装置から発行される証明書をシステムに搭載する場合に、簡単で、かつ柔軟な失効方法を備えた、証明書管理方法を提供することができる。

【発明を実施するための最良の形態】

【0024】

本発明の一実施形態について説明する。なお、これにより本発明が限定されるものではない。

【0025】

図1は、本発明の一実施形態が適用された証明書管理システムのネットワーク構成図である。

【0026】

本実施形態の証明書管理システムは、図1に示すように、複数のサービス提供者装置40₁～40_n（以下、単にサービス提供者装置40とも称する）と、クライアント端末20（以下、単に端末20とも称する）とがインターネットなどの通信網30を介して、互いに接続されて構成されている。また端末20は、ICカード10と接続される。またサービス提供者装置40₁～40_nは、それぞれ認証局装置50₁～50_n（以下、単に認証局装置50とも称する）と接続されている。

【0027】

認証局装置50は、証明書の発行申請に基づき、証明書を発行し、また、証明書の失効申請に基づき、証明書失効情報を配布する。図2に示すように、認証局装置50は、証明書を生成するための秘密鍵A501と、該秘密鍵に対応した公開鍵証明書A502と、証明書の発行申請に基づき、証明書を生成する証明書生成部502と、証明書の失効申請に基づき、証明書の失効情報を生成する失効情報生成部503と、該失効情報生成部で生成した失効情報を保管する失効情報DB504と、データの送受信を行う通信部501と、秘密鍵と該秘密鍵に対応する公開鍵を生成する鍵生成部505と、他の装置に対して証明書発行を依頼するための証明書発行申請を生成する証明書発行申請生成部506と、を含む。

【0028】

サービス提供者装置 40 は、提示された証明書の有効性を検証し、有効性検証が正しく行えた場合に、サービスを提供する。図 3 に示すように、サービス提供者装置 40 は、提示された証明書の有効性を検証する証明書検証部 402 と、該証明書検証部により、有効性検証が正しく行えた場合に、サービスを提供するサービス提供部 403 と、データの送受信を行う通信部 401 と、を含む。

【0029】

IC カード 10 は、上記サービス提供者 40 毎の固有の領域を持ち、該領域に、上記サービス提供者 40 の情報を保持し、また、証明書の発行要求に基づき、証明書を発行する。図 4 に示すように、IC カード 10 は、上記サービス提供者 40₁ ~ 40_n の情報を保持するサービス提供者固有領域 103₁ ~ 103_n（以下、サービス提供者固有領域 103 とも称する）と、証明書の発行要求に基づき、上記サービス提供者固有領域 103 に保持されている秘密鍵を用いて、証明書を発行する証明書生成部 102 と、外部とデータを送受信するデータ送受信部 101 と、秘密鍵と公開鍵のペアを生成する鍵生成部 104 と、秘密鍵を用いて暗号化を行う暗号化部 105 と、上記サービス提供者固有領域 103 に対応する上記サービス提供者装置 40 を認証し、該サービス提供者装置 40 のみにアクセスを許可するサービス提供者認証部 106 と、を含む。

【0030】

端末 20 は、上記サービス提供者装置 40 からの要求を上記 IC カード 10 に伝送し、また、上記 IC カード 10 から情報を引き出し、上記サービス提供者装置 40 に、該情報を伝送する。なお、サービス提供者固有領域 103₁ ~ 103_n との情報伝達は、上記サービス提供者認証部 106 のアクセス制御機能により、それぞれ対応するサービス提供者装置 40₁ ~ 40_n しか実行できない。

【0031】

図 5 に示すように、端末 20 は、上記 IC カード 10 とデータを送受信する IC カードアクセス部 201 と、上記サービス提供者装置 40 と、あるいは、上記認証局装置 50 と、データを送受信するデータ送受信部 202 と、を含む。

【0032】

図 6 は端末 20 のハードウェア構成図である。端末 20 は、通信装置 21 と、入出力装置 22 と、IC カード入出力装置 23 と、記憶装置 24 と、CPU 25 とメモリ 26 と、読取装置 27 とがバスなどの内部通信線 29 で連結され、記憶媒体 28 を含めて構成されている。また、端末 20 は IC カード入出力装置 23 を経由して、IC カード 10 とつながる。

【0033】

サービス提供者装置 40 および認証局装置 50 のハードウェア構成は端末 20 のハードウェア構成と同様である。ただし、サービス提供者装置 40 および認証局装置 50 が、直接 IC カード 10 へのアクセスを行わない場合は、IC カード入出力装置 23 は備えなくても良い。

【0034】

図 7 は IC カード 10 のハードウェア構成図である。IC カード 10 は、入出力部 11 と、CPU 12 と、耐タンパー記憶装置 13 と、耐タンパーメモリ 14 と、がバスなどの内部通信線 15 で連結されて構成されている。

【0035】

本実施形態の証明書管理システムにおける処理フローについて説明する。以下に述べる処理フローは、各装置の記憶装置に格納されたプログラムがメモリにロードされ、CPU により実行されることにより、証明書管理システムを構成する各装置、IC カード上に具現化される各処理部により実行されるものである。また、各プログラムは予め記憶装置に格納されても良いし、他の記憶媒体または通信媒体（ネットワークまたはネットワークを伝搬する搬送波）を介して、必要なときに導入されても良い。

【0036】

図 8 は、第 1 のサービス提供者装置 40₁ が信頼する認証局装置 50₁ が IC カード 1

0 に対して証明書を発行した後で、第 2 のサービス提供者装置 402 が信頼する認証局装置 502 が IC カード 10 に対して証明書を発行するフロー図である。

【0037】

なお、第 1 のサービス提供者装置 401 が信頼する認証局装置 501 が IC カード 10 に対して証明書を発行した後では、IC カード内で生成した秘密鍵 A1011 と公開鍵 A1021 のペア、および、該公開鍵 A1021 に対して、第 1 のサービス提供者装置 401 が信頼する認証局装置 501 が自身の秘密鍵 A5011 を用いて発行した証明書 A5031、および、認証局装置 501 自身の秘密鍵 A5011 に対応する自身の証明書 A5021 と、が、IC カード内の第 1 のサービス提供者装置 401 の領域に保存されている。

【0038】

認証局装置 502 において、上記鍵生成部 505 は、秘密鍵 A5052 と公開鍵 A5062 のペアを生成する（ステップ S401）。

【0039】

上記証明書発行申請生成部 506 は、IC カード 10 に対する証明書の発行申請を生成し、申請情報 A5072 と上記公開鍵 A5062 を IC カードに送信する（ステップ S402）。

【0040】

IC カード 10 において、証明書生成部 102 は、上記秘密鍵 A1011 を用いて認証局 502 の証明書 A5082 を生成する（ステップ S403）。

【0041】

証明書生成部 102 は、上記証明書 A5031 と、上記証明書 A5021 と、上記ステップ S403 で生成した証明書 A5082 を、データ送受信部 101 を介して認証局装置 502 に送信する。その後、端末 20 は、IC カード 10 に対して、サービス提供者装置 402 の領域を選択する（ステップ S404）。

【0042】

端末 20 は、IC カード 10 に対して秘密鍵および公開鍵ペアの生成を依頼する（ステップ S405）。

【0043】

IC カード 10 において、上記鍵生成部 104 は、秘密鍵 A1012 および公開鍵 A1022 を生成し、上記ステップ S404 で選択された領域に保存する（ステップ S406）。

【0044】

IC カード 10 の鍵生成部 104 は、データ送受信部 101 を介して、端末 20 に、上記生成した公開鍵 A1022 を送信する。端末 20 は、上記公開鍵 A1022 と、証明書申請情報 A2012 と、を認証局装置 502 に送信する（ステップ S407）。

【0045】

認証局装置 502 において、上記証明書生成部 502 は、上記ステップ S403 で、IC カードから発行された上記証明書 A5082 に対応した秘密鍵 A5052 を用いて証明書 A5092 を生成する（ステップ S408）。

【0046】

認証局装置 502 において、通信部 501 は、該証明書 A5092 と、上記ステップ S403 で、IC カードから受信した上記証明書 A5082 と、上記証明書 A5031 と、上記証明書 A5021 と、を端末 20 に送信し、端末 20 は、これらの証明書を受け取り IC カード 10 に書き込む（ステップ S409）。

【0047】

IC カード 10 のデータ送受信部 101 は、受け取った、上記各証明書をステップ S404 で選択された領域に保存する（ステップ S410）。

【0048】

なお、ステップ S403 で発行する証明書には、公開鍵 A5062 以外にも、IC カード情報や個人情報などの情報を含むようにしても良い。

【0049】

また、ステップS406で秘密鍵A101₂ および公開鍵A102₂ を、ICカード10で生成するようにしているが、認証局装置50₂ で生成し、ICカード10内に保存するようにしても良い。

【0050】

図9は、第2のサービス提供者装置40₂ が信頼する認証局装置50₂ が、ICカード10に対して発行した証明書A509₂ を検証するフロー図である。

【0051】

端末20からサービス提供要求を受けたサービス提供者装置40₂ において、上記証明書検証部402は、チャレンジ（たとえば乱数）A401₂ を生成し、端末20に送信し、証明書要求を行う（ステップS501）。

【0052】

端末20は、ICカード10に対して、サービス提供者装置40₂ の領域を選択する（ステップS502）。

【0053】

端末20は、上記ステップS501でサービス提供者装置40₂ から送られたチャレンジA401₂ を、ICカード10に送り暗号化を依頼する（ステップS503）。

【0054】

ICカード10において、上記暗号化部105は、上記S502で選択された領域に保存されている秘密鍵A101₂ で、チャレンジA401₂ を暗号化する（ステップS504）。

【0055】

ICカード10のデータ送受信部101は、上記ステップS504で暗号化されたチャレンジA402₂ と、上記ステップS504の暗号化で使用した秘密鍵A101₂ に対応した証明書A509₂ と、該証明書A509₂ の発行に使用した秘密鍵に対応した認証局装置50₂ の証明書A508₂ と、該証明書A508₂ の発行に使用したICカード内の秘密鍵に対応した証明書A503₁ と、上記証明書A502₁ と、を端末20に送信する。

【0056】

端末20は、ICカード10から受け取った、暗号化されたチャレンジA402₂ と、上記各証明書と、をサービス提供者装置40₂ に転送する（ステップS505）。

【0057】

サービス提供者装置40₂ において、上記証明書検証部402は、受け取った証明書A509₂ を使って、暗号化されたチャレンジA402₂ を復号化し、上記ステップS501で送信したチャレンジA402₂ と一致するかどうかを確認しチャレンジの検証を行う（ステップS506）。

【0058】

サービス提供者装置40₂ において、上記証明書検証部402は、受け取った上記各証明書が失効されていないかどうかを確認するために、認証局装置50₁ および、認証局装置50₂ に対して証明書の失効情報の取得処理を行う（ステップS507）。

【0059】

認証局装置50₁ および認証局装置50₂ は、ICカード10の利用者からの連絡に基づいて随時更新される上記失効情報DB504に基づいて、上記失効情報生成部503において失効情報を生成している。ステップ507における失効情報の要求に従い、証明書の失効情報を通知する（ステップS508）（ステップS509）。

【0060】

サービス提供者装置40₂ において、上記証明書検証部402は、上記各証明書の検証処理を行う（ステップS510）。

【0061】

検証に成功し、証明書は有効である、と判断した場合、上記サービス提供部403は、

サービスの提供を行う（ステップ S 5 1 1）。

【0062】

なお、ステップ S 5 1 0 において、証明書検証部 4 0 2 自らが証明書を検証しているが、外部の証明書検証機関に、検証を行いたい証明書を送信し、証明書の有効性の問い合わせをするようにしても良い。

【0063】

図 1 0 は、上記証明書検証ステップ（S 5 1 0）を詳細に説明するためのフロー図である。

【0064】

上記認証局装置 5 0 2 が発行した証明書 A 5 0 9 2 の有効性の検証を行う（ステップ S 6 0 1）。具体的には上記ステップ S 5 0 8 で通知された失効情報 A 5 0 4 2 に失効された記載が無いか確認するとともに、上記証明書 A 5 0 9 2 を発行するときに使用した秘密鍵に対応した認証局装置 5 0 2 の証明書 A 5 0 8 2 に含まれる公開鍵を使用し、上記証明書 A 5 0 9 2 に記述されているデジタル署名を検証する。失効されていない、かつ、デジタル署名が有効である、ならば次のステップを実行する。そうでなければ、証明書 A 5 0 9 2 は無効であると判断する。

【0065】

上記 IC カード 1 0 が発行した証明書 A 5 0 8 2 の有効性の検証を行う（ステップ S 6 0 3）。具体的には上記ステップ S 5 0 8 で通知された失効情報 A 5 0 4 2 に失効された記載が無いか確認するとともに、上記証明書 A 5 0 8 2 を発行するときに使用した秘密鍵に対応した認証局装置 5 0 1 が、IC カードに対して発行した証明書 A 5 0 3 1 に含まれる公開鍵を使用し、上記証明書 A 5 0 8 2 に記述されているデジタル署名を検証する。失効されていない、かつ、デジタル署名が有効である、ならば次のステップを実行する。そうでなければ、上記証明書 A 5 0 8 2 は無効であり、同時に証明書 A 5 0 9 2 は無効であると判断する。

【0066】

上記認証局装置 5 0 1 が発行した証明書 A 5 0 3 1 の有効性の検証を行う（ステップ S 6 0 5）。具体的には上記ステップ S 5 0 9 で通知された失効情報 A 5 0 4 1 に失効された記載が無いか確認するとともに、上記証明書 A 5 0 3 1 を発行するときに使用した秘密鍵に対応した認証局装置 5 0 1 の証明書 A 5 0 2 1 に含まれる公開鍵を使用し、上記証明書 A 5 0 3 1 に記述されているデジタル署名を検証する。失効されていない、かつ、デジタル署名が有効である、ならば次のステップを実行する。そうでなければ、上記証明書 A 5 0 3 1 は無効であり、同時に上記証明書 A 5 0 8 2 は無効であり、同時に証明書 A 5 0 9 2 は無効であると判断する。

【0067】

上記認証局装置 5 0 1 が発行した証明書 A 5 0 2 1 の有効性の検証を行う（ステップ S 6 0 7）。上記ステップ S 5 0 9 で通知された失効情報 A 5 0 4 1 に失効された記載が無いか確認する。証明書 A 5 0 2 1 は、サービス提供者装置 4 0 2 が信頼する認証局装置の証明書なので、証明書 A 5 0 2 1 が失効されていなければ、証明書 A 5 0 2 1 は有効であると判断し、同時に

上記証明書 A 5 0 3 1 は有効であり、上記証明書 A 5 0 8 2 は有効であり、同時に証明書 A 5 0 9 2 は有効であると判断する（ステップ S 6 0 9）。

【0068】

そうでなければ、証明書 A 5 0 2 1 は無効であると判断し、同時に上記証明書 A 5 0 3 1 は無効であり、上記証明書 A 5 0 8 2 は無効であり、同時に証明書 A 5 0 9 2 は無効であると判断する（ステップ S 6 1 0）。

【0069】

なお、上述の各有効性確認ステップ（S 6 0 1、S 6 0 3、S 6 0 5、S 6 0 7）の順序は入れ替えても良い。

【0070】

上述のように、本実施例では、証明書A509₂の有効性を検証するためには、証明書A508₂および証明書A502₁の有効性の検証が必要となるように、証明書の連鎖を構成している。この連鎖構造により、ICカードを無くした等、何らかの理由により、証明書A509₂および証明書A502₁を失効させたい場合、上位の証明書A502₁を失効させる処理を行えば、証明書A509₂を失効させる処理を行わなくても、証明書A509₂も失効させることができる。

【0071】

一方、各証明書の検証時には、その発行元認証局が発行した失効情報A504₁とA504₂を参照するように構成している。この構成により、証明書A509₂および／または証明書A502₁を個々に失効させることも可能である。例えば、サービス提供者装置40₂が提供するサービスを停止する場合などには、サービス提供者装置40₂が信頼する認証局装置による失効情報を発行させればよい。これにより、サービス提供者装置40₁が信頼する認証局装置50₁が発行した証明書は有効のまま、サービス提供者装置40₂が信頼する認証局装置50₂から発行された証明書A509₂を失効させることが可能となる。

【0072】

なお、本発明は、上記の本実施形態に限定されるものではなく、その要旨の範囲内で様々な変形が可能である。

【0073】

たとえば、認証局装置から発行された証明書、および、認証局装置の証明書を、ICカード内に保存するようにしているが、たとえばディレクトリサーバのようなICカード外のサーバ装置を証明書保管機関装置として設けて、証明書を保管するようにしてもよい。その場合には、図8および図9で示したフローで証明書を送りあう代わりに、証明書保管機関装置の保管場所の情報を送りあうようにすれば良い。また、送りあう情報を暗号化するようにしても良い。

【0074】

また、ICカード10の内部データは、暗号化されて保存するようにしても良い。

【0075】

また、本実施例では、第2の証明書(A509₂)を発行するのは、第2のサービス提供者装置40₂が信頼する認証局装置50₂としているが、第1のサービス提供者装置40₁が信頼する認証局装置50₁が、第2の証明書(A509₂)を発行しても良い。

【0076】

また、本実施例の応用例として、複数のサービス提供者装置40_n ($n \geq 2$) がサービスを提供するために、ICカード10が、上位の認証局装置である第1の認証局装置50₁が発行した証明書A503₁と対応する秘密鍵A101₁とを用いて、複数の下位の認証局である第n ($n \geq 2$) の認証局装置50_nの証明書A508_nを生成し、さらに、該証明書A508_nと対応する秘密鍵A505_nとを用いて、第nの認証局装置50_nが証明書A509_nを発行するように構成しても良い。

【0077】

また、第m ($m \geq 2$) の認証局装置50_mが発行した証明書A503_mと対応する秘密鍵A101_mとを用いて第n ($n > m$) の認証局装置50_nの証明書A508_nを生成し、さらに、該証明書A508_nと対応する秘密鍵A505_nとを用いて、第nの認証局装置50_nが証明書A509_nを発行するようにしても良い。

【図面の簡単な説明】

【0078】

【図1】 本発明の一実施形態が適用された証明書管理システムのネットワーク構成を説明するための図である。

【図2】 認証局装置の構成例を示すための図である。

【図3】 図1に示すサービス提供者装置の構成例を示すための図である。

【図 4】 図 1 に示す IC カードの構成例を示すための図である。

【図 5】 図 1 に示す端末の構成例を示すための図である。

【図 6】 図 1 に示す端末のハードウェア構成を示す図である。

【図 7】 図 1 に示す IC カードのハードウェア構成を示す図である。

【図 8】 本発明の一実施形態が適用された証明書管理システムの証明書発行を説明するフロー図である。

【図 9】 本発明の一実施形態が適用された証明書管理システムの証明書検証を説明するフロー図である。

【図 10】 図 9 の証明書検証ステップを詳しく説明するフロー図である。

【符号の説明】

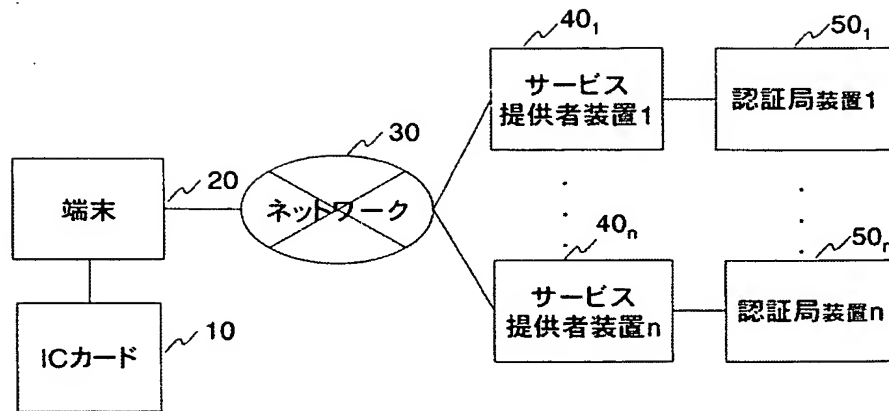
【0079】

10・・・ICカード, 11・・・入出力装置, 12・・・CPU, 13・・・記憶装置, 14・・・メモリ, 15・・・内部通信線, 20・・・端末, 21・・・通信装置, 22・・・入出力装置, 23・・・ICカード入出力装置, 24・・・記憶装置, 25・・・CPU, 26・・・メモリ, 27・・・読取装置, 28・・・記憶媒体, 29・・・内部通信線, 30・・・ネットワーク, 40₁～40_n・・・サービス提供者装置, 50₁～50_n・・・認証局装置, 101・・・データ送受信部, 102・・・証明書生成部, 103₁～103_n サービス提供者固有領域, 104・・・鍵生成部, 105・・・暗号化部, 106・・・サービス提供者認証部, 201・・・ICカードアクセス部, 202・・・データ送受信部, 401・・・通信部, 402・・・証明書検証部, 403・・・サービス提供部, 501・・・通信部, 502・・・証明書生成部, 503・・・失効情報生成部, 504・・・失効情報データベース, 505・・・鍵生成部, 506・・・証明書発行申請生成部, A101₁・・・秘密鍵, A101₂・・・秘密鍵, A102₁・・・公開鍵, A102₂・・・公開鍵, A201₁・・・申請情報, A201₂・・・申請情報, A502₁・・・認証局装置50₁の証明書, A503₁・・・認証局装置50₁発行の証明書, A401₁・・・チャレンジ, A401₂・・・チャレンジ, A402₁・・・暗号化されたチャレンジ, A402₂・・・暗号化されたチャレンジ, A504₁・・・失効情報, A504₂・・・失効情報, A505₂・・・秘密鍵, A506₂・・・公開鍵, A507₂・・・申請情報, A508₂・・・A503₁に対応した秘密鍵で生成した証明書, A509₂・・・認証局装置50₂発行の証明書。

【書類名】 図面

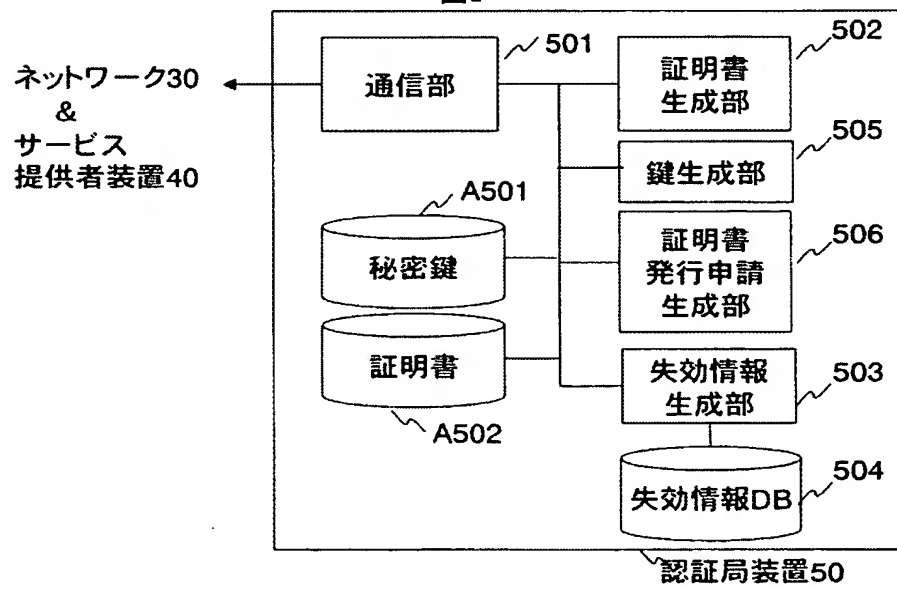
【図 1】

図1



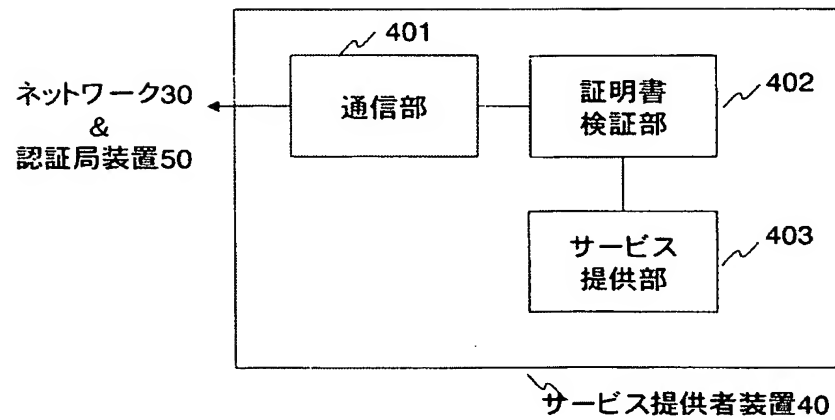
【図 2】

図2



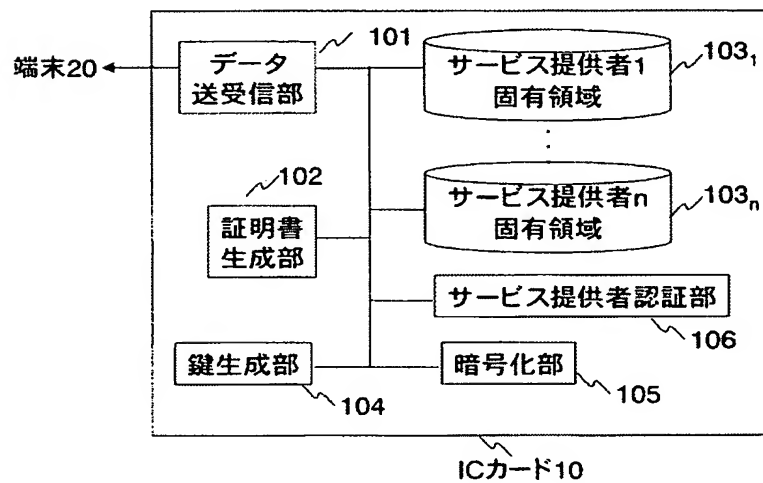
【図 3】

図3



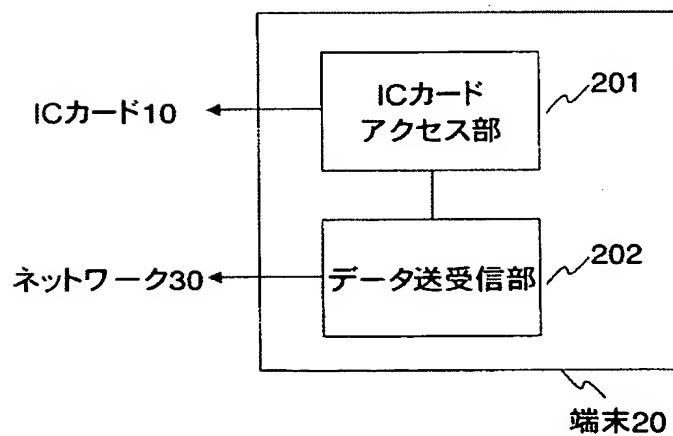
【図 4】

図4

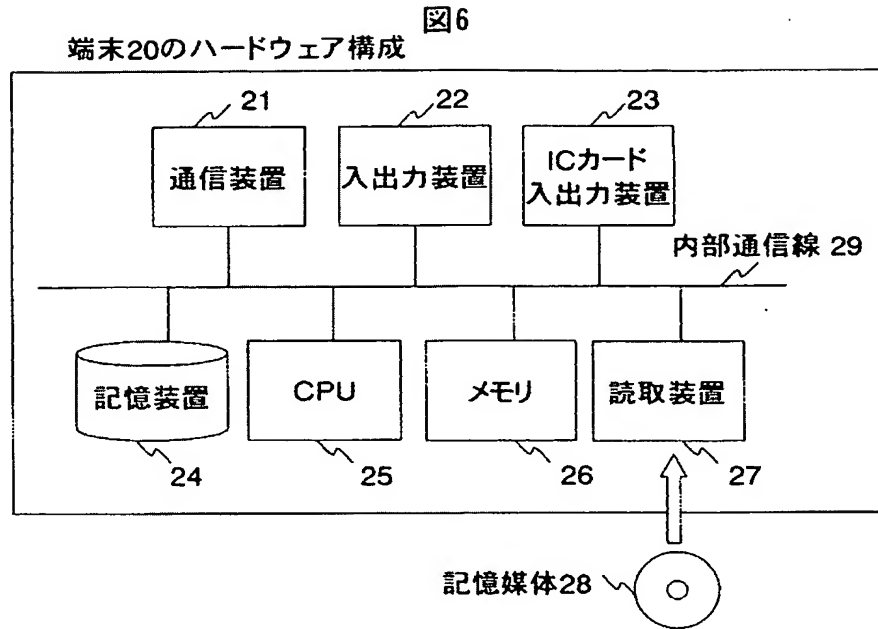


【図 5】

図5



【図 6】



【図 7】

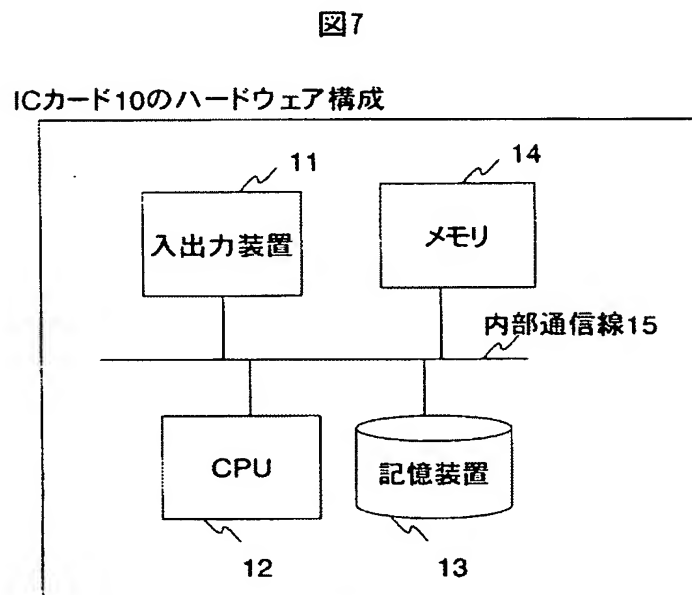
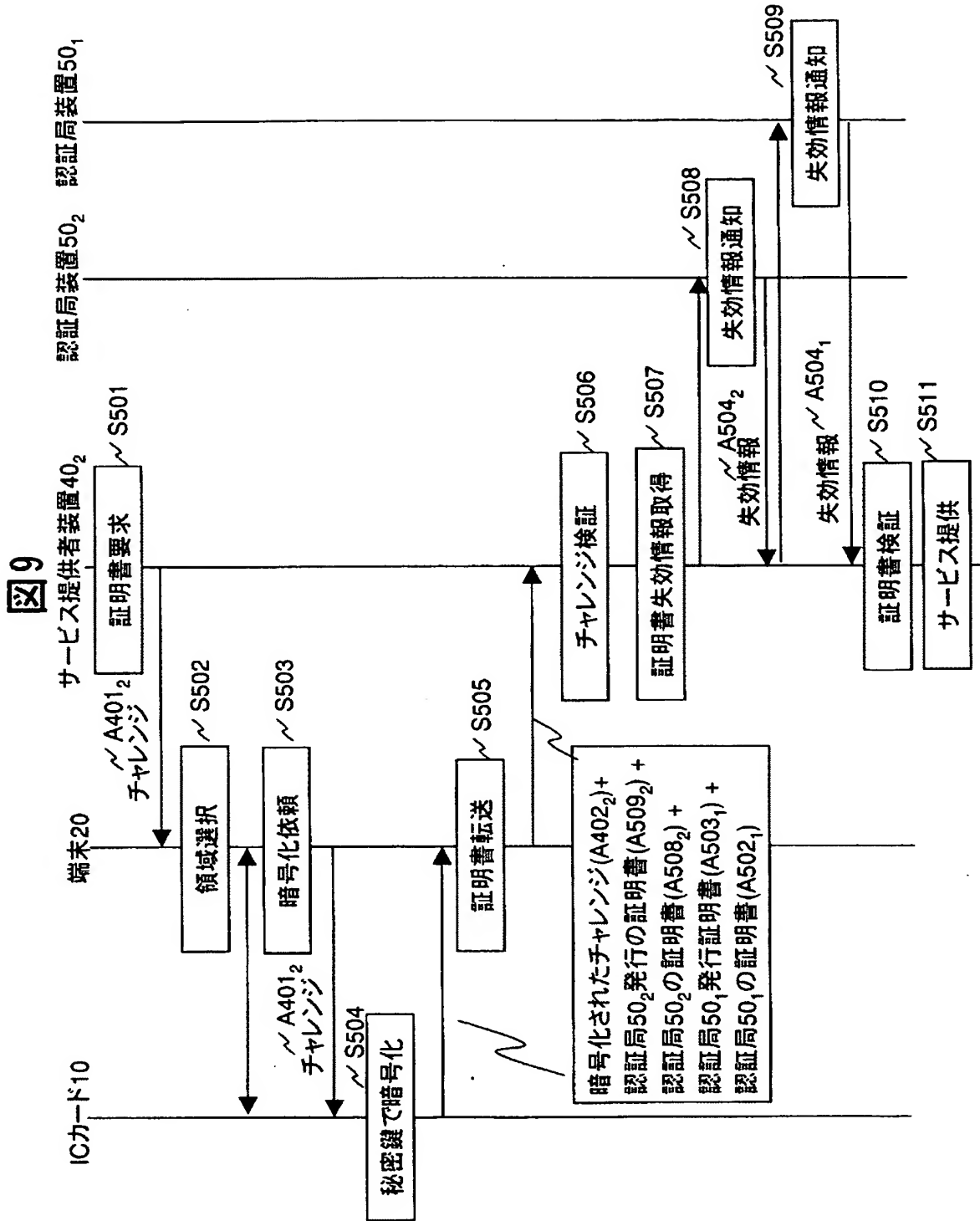
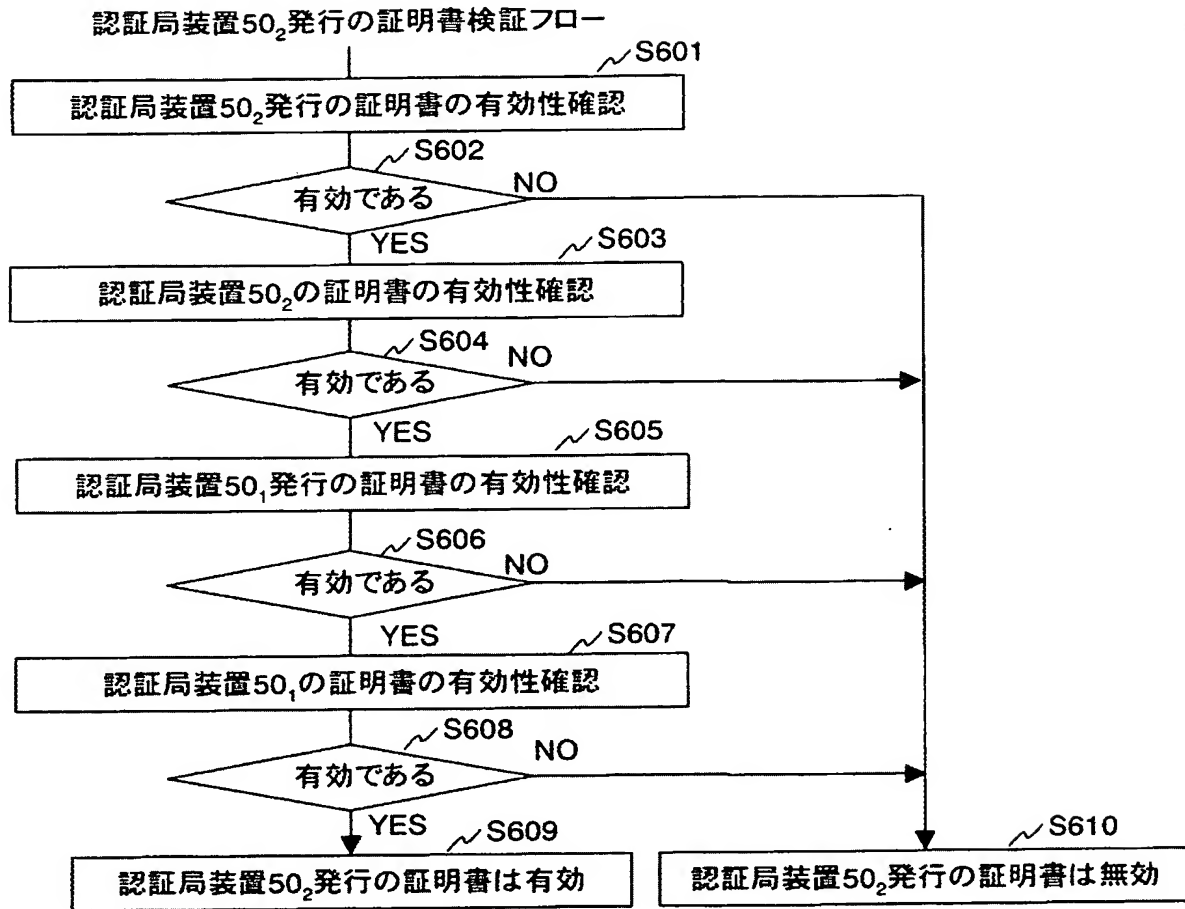


図 9



【図 10】

図10



【書類名】 要約書**【要約】****【課題】**

複数のサービス提供者装置が、それぞれ異なる信頼する認証局装置から発行される証明書を、ICカードに搭載される場合に、第一のサービス提供者装置が信頼する認証局装置が発行した証明書を失効させるだけで、すべての証明書を失効させることができ、また、個々の証明書を個別に失効させることができる、証明書管理方法およびその方法が適用されるシステムを提供する。

【解決手段】

認証局 n ($n \geq 2$) は、ICカードに事前に搭載済みの認証局 1 から発行された証明書 1 と対応する秘密鍵 1 を用いて生成された証明書 n' と対応する秘密鍵 n' を用いて、証明書 n を発行する。すべての証明書を失効させたい場合は、認証局 1 から発行された証明書 1 を失効させる。

【選択図】 図 4

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 4 0 2 4 0 1
受付番号	5 0 3 0 1 9 8 2 4 4 1
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 5 年 1 2 月 3 日

< 認定情報・付加情報 >

【提出日】 平成 15 年 12 月 2 日

特願 2 0 0 3 - 4 0 2 4 0 1

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 1 0 8]

1. 変更年月日	1 9 9 0 年 8 月 3 1 日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台 4 丁目 6 番地
氏 名	株式会社日立製作所